The Surveillance Iceberg: Mass Spying under the FISA Amendments Act

History teaches that government spying is naturally subject to abuse without strong oversight, yet only the tiniest fraction of electronic surveillance of Americans—the tip of a vast and rapidly growing iceberg—is meaningfully visible today. Under the controversial Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA) of 2008, set to expire at the end of the year, the National Security Agency (NSA) is empowered to vacuum up the international communications of Americans under sweeping authorizations that dispense with the need for individual warrants. Despite reports of large-scale overcollection of Americans' emails and phone calls, the NSA has brazenly refused to give Congress any estimate of how many citizens' private conversations are being captured in its vast databases. At a Cato Policy Forum held in July, Julian Sanchez, research fellow at the Institute, took a closer look behind this veil of secrecy. Sen. Ron Wyden (D-OR), who has blocked unanimous consent requests to pass a five-year extension of the FAA, offered his hopes for establishing sorely needed accountability when it comes to surveillance.

JULIAN SANCHEZ: It is a truism of the information age that knowledge is power. Here at Cato, however, we always try to be cognizant of Lord Acton's famous warning about what power tends to do. Unfortunately, the history of the American intelligence community demonstrates all too clearly that, at least in government hands, data tends to corrupt—and massive databases corrupt massively.

Both our own experience and that of less free societies around the world have made it apparent that a government's ability to monitor its citizens' private communications is among its most dangerous powers. Without strong oversight, it is highly susceptible to abuse. Yet, while we recognize accountability to the public as one of the strongest checks against abuse of surveillance power, several factors have vastly increased the amount of unaccountable monitoring by intelligence agencies in recent years.

In the decades prior to the passage of the Foreign Intelligence Surveillance Act of 1978, the Federal Bureau of Investigation and other government agencies systematically and illegally spied on American antiwar activists, legislators, Supreme Court justices, political advisers, members of Congress, at least one first lady and civil rights leaders—including, perhaps most notoriously, the Rev. Martin Luther King Jr. As we now know, the FBI hoped he could be discredited or driven to suicide and replaced with what they termed "the right kind of negro leader"—one who would be covertly answerable to the Bureau itself.

None of this illegally obtained information ever saw the inside of a court, where it might be challenged. Instead, it was deployed through selective, targeted leaks of information to friendly politicians and journalists—effectively escaping any kind of real public accountability.

As these abuses came to light, thanks to the investigative work of the Church Committee in the 1970s, Congress began to realize that the corrupting power of surveillance required the counterbalancing force of oversight. This would come first and foremost from judges, but also, to the extent possible, from Congress and the public.

Much as the Cold War provided the context for surveillance abuses in the 1960s and 1970s, the attacks of September 11th set the stage for a new era of massive surveillance with minimal accountability. Many different factors have contributed to that trend. One is the fear that, without flexibility and rapid action unencumbered by judicial oversight, American intelligence agents won't be able to respond quickly enough to the threat of terror. Another is the advent of new technologies that have enabled new types of surveillance, even in ordinary criminal investigations. which don't trigger the traditional statutory reporting or warrant requirements,—surveillance of stored electronic records and emails, for instance, doesn't trigger the same reporting obligations as a traditional phone wiretap. At the same time, new technologies have greatly expanded the ability of intelligence agencies to vacuum up and sift through an ever-growing torrent of communications data.

Every year, the Administrative Office of the U.S. Courts releases a thick, data-rich report on criminal wiretaps. There's also a much shorter public report issued by the Justice Department on secret FISA surveillance. There are still, however, vast quantities of additional information-gathering about which we know almost nothing. That includes the FISA Amendments Act of 2008. The National Security Agency and the Justice Department have refused to tell even Congress how many Americans have been swept into its vast databases of information collected under this legislation. Each day, those databases are growing ever larger. We do know that in Utah a massive data storage facility is being constructed that former NSA officials have said could be effectively used to store the total volume of international data communications.

The scale of this information itself is a barrier to meaningful oversight. An audit in 2008 found that the FBI alone had over a century's worth of backlogged FISA record-

ings. The NSA has much, much more. As James Clapper, the director of national intelligence, has said, "There's only one entity in the entire universe that has visibility on all Special Access Programs—that's God." Unfortunately, what we have instead is Congress.

Given their limited access and resources, including a relatively small number of staffers with both clearance and relevant legal expertise, members of Congress have little incentive to expend energy and political capital fixing problems with secret surveillance. Even if they succeed, after all, they won't be able to put out a press release trumpeting the achievement. Especially in an election year, the attitude of many congressional overseers is exemplified by a comment made by Sen. Leverett Saltonstall (R-MA) in 1956. He said that the issue wasn't so much the reluctance of the intelligence agencies to talk to Congress, but, as he put it, "our reluctance to seek information and knowledge on subjects which I personally, as a member of Congress and as a citizen, would rather not have."

We are fortunate to have a radically different attitude represented in Congress today in the person of Sen. Ron Wyden. Please join me in welcoming today's speaker.

SEN. RON WYDEN: Let me begin with some background. If a law enforcement agency has compelling evidence that an American citizen is a serious criminal, the officers can get a warrant from a judge to tap that individual's phone. This procedure—based on probable cause—is built upon the Fourth Amendment, which the Founding Fathers considered sacred ground. It was a bedrock principle that the government could not violate the privacy of Americans with unreasonable searches and seizures. And it was a brilliant concept, simultaneously protecting individual privacy while setting up procedural mechanisms in the face of threats to public safety.

In 1978, Congress passed the Foreign Intelligence Surveillance Act, which governs wiretapping for intelligence purposes. If there is evidence that a person is a spy or a member of an international terrorist group, this legislation allowed the government to procure a warrant, even if that person had not yet committed a crime. It was based on the same concepts as probable cause, and it continues to be used today.

After September 11th, however, the Bush administration decided that it needed additional surveillance authorities beyond the FISA statute. Instead of engaging Congress, however, it manufactured a warrantless wiretapping program that operated in secret for a number of years. This, like everything else, eventually became public. There was a huge uproar, both within the halls of Congress and beyond. After a passionate national debate, Congress passed the FISA Amendments Act of 2008, replacing the warrantless wiretapping program with new government authorities to collect the phone calls and emails of those believed to be foreigners outside of the United States.


Julian Sanchez

> "At least in government hands, data tends to corrupt—and massive databases corrupt massively."

The centerpiece of that Act, and a big part of my concern, is a provision that has come to be known as Section 702. This provision, unlike the traditional FISA authorities, allows the government to collect foreign communications without individual warrants. It also contains language specifically intended to limit the government's ability to deliberately spy on law-abiding Americans. Congress put an expiration date on these new authorities, designed to foster ongoing and continuous review, and the next expiration date is in December.

The question, therefore, is whether the FISA Amendments Act should remain as it stands or whether it needs reform. For the last 18 months, Sen. Mark Udall (D-CO) and I have been asking questions. Because Section 702 was targeted at people outside our borders, it is particularly important for the public to get a rough understanding of how many people inside the United States have had their private communications collected under these authorities. If only a handful have had their phone calls and emails collected, there is probably not a substantial threat to privacy rights. But if the number is significant, then that would suggest that the privacy protections of American citizens need to be strengthened.

So we asked for an estimate. The Office of the Director of National Intelligence told the two of us in July 2011 that "it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed'' under the Act. Obviously, this wasn't a particularly helpful response. I am prepared to accept that it might be difficult to come up with an exact count of this number, but it is hard for me to believe that it is impossible to even estimate it.

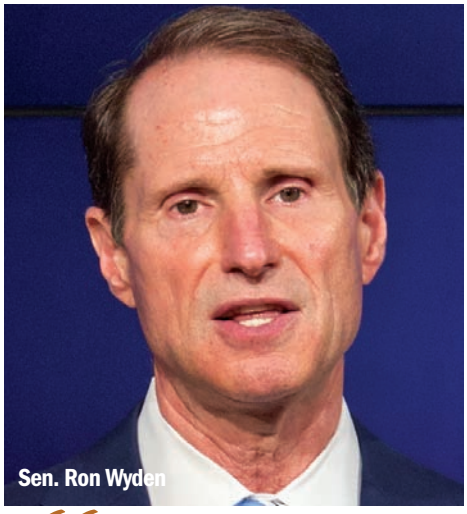
This June, in one of the more remarkable statements I've heard in my time in public service, the leadership of the NSA said that trying to come up with this estimate would in itself violate the privacy of U.S. persons. Even by Washington standards, this was farfetched. How exactly does it violate privacy rights to give a ballpark estimate of how many people have had their communications swept up?

I am concerned, of course, that if no one has even estimated how many Americans have had their communications collected under the FISA Amendments Act, then it is

possible that this number could be quite large. Since all of the communications collected by the government under section 702 are collected without individual warrants, I believe that there should be clear rules prohibiting the government from searching through these communications in an effort to find the phone calls or emails of a particular American, unless the government has obtained a warrant or emergency authorization permitting surveillance of that American.

Another concern is that if the government wants to search its collected communications in order to find a particular American's communications, there is currently no requirement to get a warrant. As it is currently written, in other words, Section 702 does not contain adequate protections against warrantless "backdoor" searches—even though they are the very thing that many people thought the FISA Amendments Act was intended to prevent. This loophole ought to be closed, as it would circumvent the traditional warrant requirements laid out in the Fourth Amendment.

I want to be clear: If the government has evidence that an American is engaged in terrorism, espionage, or other serious crimes, officials should be able to read that person's emails and listen to their phone calls. In fact, I believe that this is an essential part of protecting our country from terrorism. Senator Udall and I offered an amendment during the committee's markup of this bill that would have clarified the law to prohibit searching through communications collected under section 702 in an effort to find a particular American's communications. We included exceptions for searches that involved a warrant or an emergency authorization, as well as for searches for the phone calls or emails of people who consent to the search.


Sen. Ron Wyden

"Searching for Americans' phone calls and emails without a warrant is something that these agencies should not do."

This amendment was voted down. However, it was offered up to the Senate Judiciary Committee by Sen. Mike Lee (R-UT). This is at least an indication that these issues are seeing a spark of life. In fact, two particularly critical developments emerged last summer in response to my request for the intelligence community to declassify certain statements. For starters, the government admitted—for the first time—that a violation of Fourth Amendment privacy rights had taken place. In addition, the Foreign Intelligence Surveillance Court decided that the use of expanded surveillance authorities "has sometimes circumvented the spirit of the law."

It's time to step back and take a closer look at these important constitutional issues. I believe that we have an obligation as elected legislators to discuss what these agencies should or should not be doing, and it is my hope that a majority of my colleagues will agree that searching for Americans' phone calls and emails without a warrant is something that these agencies should not do. The founding fathers got it right. We need to strike a better balance between individual liberty and collective security. ■